Insight Assurance

SOC 2| ISO 27001 | PCI | HIPAA

System and Organization Controls (SOC 3)
Report on Fluid Attacks Inc.’s Application Security Solutions
System Relevant to Security
For the Period March 4, 2024, to June 3, 2024

fluid attacks

we hack your software

TABLE OF CONTENTS

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR’S REPORT ON A SOC 3 EXAMINATION

To: Fluid Attacks Inc.

Scope

We have examined Fluid Attacks Inc.’s (‘Fluid Attacks’) accompanying assertion titled “Fluid Attacks Inc.’s Management Assertion” (assertion) that the controls within Fluid Attacks’ Application Security Solutions System (system) were effective throughout the period March 4, 2024, to June 3, 2024, to provide reasonable assurance that Fluid Attacks’ service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022) in* AICPA, *Trust Services Criteria*.

Service Organization’s Responsibilities

Fluid Attacks is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Fluid Attacks service commitments and system requirements were achieved. Fluid Attacks has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Fluid Attacks is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion, based on our examination, on management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements.

- Assessing the risks that controls were not effective to achieve Fluid Attacks' service commitments and system requirements based on the applicable trust service criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Fluid Attacks' service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Fluid Attacks' Application Security Solutions System were effective throughout the period March 4, 2024, to June 3, 2024, to provide reasonable assurance that Fluid Attacks' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Insight Assurance LLC

Tampa, Florida
July 16, 2024

FLUID ATTACKS INC.’S MANAGEMENT ASSERTION

fluid
attacks
we hack your software

FLUID ATTACKS INC.’S MANAGEMENT ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Fluid Attacks Inc.’s (‘Fluid Attacks’) Application Security Solutions System throughout the period March 4, 2024, to June 3, 2024, to provide reasonable assurance that Fluid Attacks’ service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022),* in AICPA *Trust Services Criteria*. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 4, 2024, to June 3, 2024, to provide reasonable assurance that Fluid Attacks’ service commitments and system requirements were achieved based on the applicable trust services criteria. Fluid Attacks’ objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period March 4, 2024, to June 3, 2024, to provide reasonable assurance that Fluid Attacks’ service commitments and system requirements were achieved based on the applicable trust services criteria.

Fluid Attacks Inc.
July 16, 2024

ATTACHMENT A
DESCRIPTION OF THE BOUNDARIES OF FLUID ATTACKS INC.’S APPLICATION SECURITY SOLUTIONS SYSTEM

ATTACHMENT A

FLUID ATTACKS INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS APPLICATION SECURITY SOLUTIONS SYSTEM

SERVICES PROVIDED

Fluid Attacks' Continuous Hacking is a solution that combines application security testing tools, artificial intelligence (AI), and a hacking team to find and help remediate security vulnerabilities throughout the software development lifecycle and ensure secure deployments.

Fluid Attacks reports risk exposure promptly to its clients and supports them to achieve high remediation rates and guarantee high-quality and safe products to their end users.

Fluid Attacks' security testing involves different automated and manual techniques, namely, static application security testing (SAST), dynamic application security testing (DAST), software composition analysis (SCA), cloud security posture management (CSPM), secure code review, manual penetration testing, and reverse engineering. Further, Fluid Attacks uses its own AI tool to sort files in a code repository by their probability of containing security vulnerabilities, thus informing Fluid Attacks' hacking team of which files to prioritize in their manual tests.

Fluid Attacks reports findings both by its tool and hacking team to its clients on Fluid Attacks' platform. There, its clients can control the remediation process, request retests to verify fixes and keep track of their progress in risk mitigation, among other vulnerability management tasks. To help developers incorporate vulnerability management into their workflow, Fluid Attacks offers integration with several tools developers often use.

Fluid Attacks' support in the vulnerability remediation process is through custom and automated fixes generated by AI from Fluid Attacks' VS Code extension. Additionally, Fluid Attacks' feature called "Talk to a Hacker," allows its clients to meet with Fluid Attacks' hacking team for guidance on remediation. Further, Fluid Attacks offers a tool to prevent the client's development team from deploying software versions with unaccepted vulnerabilities, thus helping to enforce its client's policies and urge the development team to fix the software security issues.

INFRASTRUCTURE

Fluid Attacks maintains a system inventory that includes virtual machines (EC2 instances), computers (laptops), and mobile devices (mobile phones). The inventory documents device name, device type, vendor function, OS, location, and notes.

The in-scope hosted infrastructure consists of multiple primary service components, as shown in the table below:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
AWS Elastic Compute Cloud (EC2)	AWS	EC2 instances are used by EKS (on-demand and spot instances) as well as EMR (spot instances).
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload and download customer data.

The Fluid Attacks application infrastructure is located at the EE.UU. East Region (Northern Virginia) and UE Region (Ireland) data centers. AWS acts as a hosting subservice organization for the company. The subservice organization provides physical security and environmental protection controls, as well as managed services for Fluid Attacks' infrastructure.

AWS's network security uses software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules.

In addition to the firewall, Fluid Attacks exerts endpoint security through Mobile Device Management (MDM), which includes antivirus and antimalware, and forbids end-users from disabling or altering software.

Fluid Attacks' Information Security Policy and security procedures ensure that all computer devices (including servers, desktops, etc.) connected to the Fluid Attacks network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed. The IT department verifies that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. In the event of a virus threat, the anti-virus system will remove or quarantine the infected file.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. Fluid Attacks performs continuous security testing to its own technology to detect potential vulnerabilities to the production environment and corporate data. Email is scanned at the gateway and in the hosted email environment. Server operating systems utilize anti-virus and anti-spyware programs. All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on Fluid Attacks-owned computers, as enforced through MDM. IT staff maintains several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible.

SOFTWARE

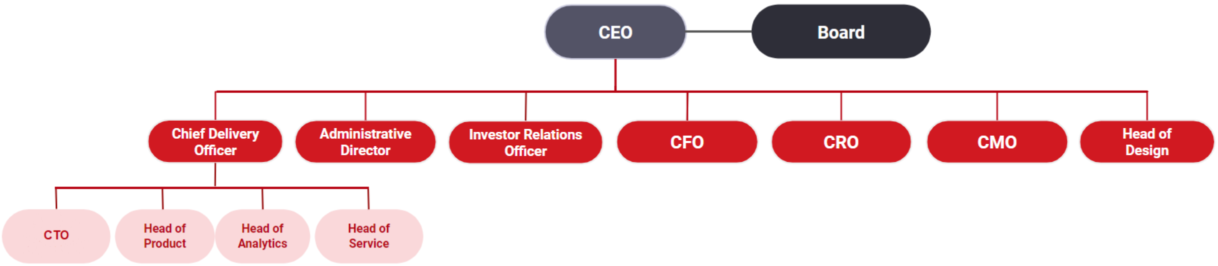
Fluid Attacks maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation. Critical software in use includes the following:

Primary Software	
System/Application	**Purpose**
Okta	Identity and access management
Cloudflare	Creating network and security solutions
Vanta	Compliance Tool
GitLab	Web-based Git repository
dbt Labs	Data transformation and analytics
Google Workspace	Communications
Nix	Building and deploying applications
Time Doctor 2	Time and track reporting
Vanta	Compliance Tool

PEOPLE

The Fluid Attacks staff provides support for the above services. Fluid Attacks employs dedicated team members to handle all major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and recovery. The company focuses on hiring the right people for the right job as well as training them both in their specific tasks and on the ways to keep Fluid Attacks and its data secure.

Fluid Attacks' corporate structure includes the following roles:



Chief Executive Officer (CEO) – Handles the strategic direction of Fluid Attacks. The CEO assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments.

Board – Provides strategic oversight, guidance, and accountability, ensuring that Fluid Attacks operates in the best interest of its shareholders and stakeholders. The Board's responsibility includes oversight of Fluid Attacks' cyber risk management.

Chief Delivery Officer – Responsible for the technological direction and advancements of the organization. Directs the product, engineering, analytics and service teams to efficiently create/present new services, maintain existing ones, and help support the Fluid Attacks customer base using the service.

Administrative Director – Responsible for administrative support and human resources, as well as for developing policies and procedures and ensuring compliance with regulations.

Investor Relations Officer – Responsible for the communication and relationships between Fluid Attacks and its investors and financial stakeholders. Their responsibilities include monitoring market trends and defining pricing models.

Chief Financial Officer (CFO) – Responsible for overseeing all financial activities and strategies to ensure Fluid Attacks' financial health and stability. Their role involves managing financial planning, budgeting, and forecasting.

Chief Revenue Officer (CRO) – Primary role for outbound reach to prospects and completing sales. They are also responsible for the maintenance and renewal of existing customer contracts.

Chief Marketing Officer (CMO) – Responsible for the outward communication of company initiatives. Primary role responsible for exposing new programs to prospects and existing customers and furthering the public reach of Fluid Attacks.

Head of Design – Responsible for developing an intuitive user experience for the Fluid Attacks platform as well as visually appealing designs for Fluid Attacks' products' user interfaces and branding.

Chief Technology Officer (CTO) – This role is responsible for the development of Fluid Attacks' platform as well as for enhancing and augmenting the capabilities of Fluid Attacks' vulnerability scanner. They are also responsible for daily IT support aspects, including support to end-users with day-to-day issues.

Head of Product – This role is responsible for the strategic vision and roadmap of Fluid Attacks' software products, guaranteeing compliance with quality, and therefore security, standards.

Head of Analytics – This role is responsible for all of Fluid Attacks analytics, providing the information for the company to make decisions supported on reliable data. Moreover, they are responsible for the ideation of the charts and metrics that are presented to end-users on Fluid Attacks' platform.

Head of Service – This role is responsible for the activities of Fluid Attacks' hacking team and managing client relationships to ultimately achieve the client's objectives in alignment with Fluid Attacks.' This role is also responsible for Fluid Attacks' research of vulnerabilities in open-source software projects.

DATA

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements or within the Fluid Attacks Knowledge Base website. Customer data is captured which is utilized by Fluid Attacks in delivering its application security solution. Data is categorized in the following major types of data usage:

Data Classification		
Category	**Category**	**Category**
Confidential	Highly sensitive data requiring the highest levels of protection has restricted access limited to specific employees or departments. The disclosure of such records to others requires explicit approval from a company executive.	● Customer Data ● Personally identifiable information (PII) ● Company financial and banking data ● Salary, compensation and payroll information ● Strategic plans ● Risk assessment reports ● Technical vulnerability reports ● Authentication credentials ● Secrets and private keys ● Litigation data
Restricted	Fluid Attacks Inc. proprietary information requiring thorough protection; access is restricted to employees with a "need-to-know" based on business requirements. This data can only be distributed outside the company with approval.	● Legal documents ● Contracts ● Internal reports ● Email and chat messages
Internal	Non-confidential information or data assets that are not intended for public disclosure can be shared internally within the company without prior approval. However, approval is necessary to share such data assets with external parties.	● Internal policies and procedures ● Employee directories ● Training materials ● Meeting minutes and internal presentations ● Publicly available industry research and news ● Non-sensitive project updates and status reports
Public	Documents intended for public consumption which can be freely distributed outside Fluid Attacks Inc.	● Marketing materials ● Product descriptions ● Release notes ● External facing policies ● Public source code

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. All employees and contractors of Fluid Attacks are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are subject to limited exceptions, confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to Fluid Attacks' business and finances are, as a matter of Fluid Attacks policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, applications and systems is shared by the IT department. IT is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under their control, moreover, Fluid Attacks personnel is required to sign a non-disclosure agreement (NDA).

Fluid Attacks has policies and procedures in place to ensure prior retention and disposal of confidential and private data. The retention and data destruction policies define the retention periods and proper destruction procedures for the disposal of data. These policies are reviewed at least annually. The destruction of data is a multi-step process. Client accounts and data are deleted upon termination of the contract.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Cloud networks are protected by enterprise-class firewalls and appropriate enterprise-class virus protection is in place. Passwords protection with assigned user rights is required for access to the network, applications, and databases. Access to the network, applications, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

PROCEDURES

Formal IT policies and procedures exist that describe logical access, computer operations, change management, incident management, and data communication standards to obtain the stated objectives for system and data security, data privacy, and integrity for both the company and its clients and define how services should be delivered. These are communicated to employees and located within the organization's intranet.

Reviews and changes to these policies and procedures are performed annually and are approved by senior management.

ATTACHMENT B
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Fluid Attacks designs its processes and procedures related to the Fluid Attacks Application Security Solutions system ("System") to meet its objectives. Those objectives are based on the service commitments that Fluid Attacks makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Fluid Attacks has established for the services.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online and in the Fluid Attacks privacy policy and terms of use.

Security Commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Regular vulnerability scans over the system and network
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal

Fluid Attacks establishes operational requirements that support the achievement of security relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies and/or procedures around how the service is designed and developed, how the system is operated, how the internal business systems and infrastructure are managed, and how employees are hired and trained. In addition, how to carry out specific manual and automated processes required in the operation and development of the System.